UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/917,368	07/27/2001	Jeffrey Scott Bardsley	RSW920010137US1	1486

7590 06/30/2010

Duke Yee
Yee & Asscoiates P C
4100 Aipha Road
Suite 1100
Dallas, TX 75244

EXAMINER	
POPHAM, JEFFREY D	
ART UNIT	PAPER NUMBER
2437	

MAIL DATE	DELIVERY MODE
06/30/2010	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS
AND INTERFERENCES

Ex parte JEFFREY SCOTT BARDSLEY,
ASHLEY ANDERSON BROCK, NATHANIEL WOOK KIM
and CHARLES STEVEN LINGAFELT

Appeal 2009-006231
Application 09/917,368
Technology Center 2400

Decided: June 30, 2010

Before KENNETH W. HAIRSTON, MARC S. HOFF
and CARL W. WHITEHEAD, JR., *Administrative Patent Judges*.

HAIRSTON, *Administrative Patent Judge*.

DECISION ON APPEAL

This is an appeal under 35 U.S.C. §§ 6(b) and 134 from the final rejection of claims 5 to 11 and 15 to 27.

The disclosed invention relates to a method and apparatus for determining a logical entry point of an attack upon a device protected by an intrusion detection system, and then identifying a physical entry point associated with the logical entry point (Fig. 1; Spec. 4-11; Abstract).

Claim 5 is representative of the claims on appeal, and it read as follows:

5. A computer-implemented method of identifying the entry point of an attack upon a device protected by an intrusion detection system, the method comprising the steps of:

obtaining intrusion information, from an intrusion detection system, regarding an attack upon a device protected by the intrusion detection system;

obtaining network information, from network equipment connected to the device, regarding the attack;

determining a logical entry point of the attack using a correlation engine to correlate the intrusion information and the network information; and

identifying a physical entry point associated with the logical entry point.

The prior art[1] relied upon by the Examiner in rejecting the claims on appeal is:

Skirmont	US 6,553,005 B1	Apr. 22, 2003
Ricciulli	US 6,973,040 B1	Dec. 6, 2005

Hunt, *Network Dispatcher: a connection router for scalable Internet services*, Internet Security Systems, Oct. 2, 1998, pp. 1-14.

[1] The filing dates of the Skirmont and the Ricciulli references are presumed to be prior to the filing date of the subject application.

The Examiner rejected claims 5 to 10, 15, and 18 to 20 under 35 U.S.C. § 102(e) based upon the teachings of Ricciulli.

The Examiner rejected claims 11, 17, and 21 to 27 under 35 U.S.C. § 103(a) based upon the teachings of Ricciulli and Skirmont.

The Examiner rejected claims 16 under 35 U.S.C. § 103(a) based upon the teachings of Ricciulli and Hunt.

The Examiner contends (Final Rej. 5) that column 3, lines 16 to 43, and column 4, line 45 to column 5, line 2 of Ricciulli describe all of the steps set forth in claim 5. In response, Appellants acknowledge (App. Br. 17) that Ricciulli's "UDP ports and TCP/IP ports are ports maintained by an operating system as logical entry points to the operating system," but argue (App. Br. 12-20) that Ricciulli determines the physical source router entry point that is the source of an attack, but does not determine a logical entry point of an attack as set forth in the claims on appeal.

The referenced portions of Ricciulli describe a method and apparatus for identifying a source of an attack upon a network node that is protected by an intrusion detection system. The method and system obtains intrusion information concerning the attack (e.g., flooding and/or denial of service) upon the protected network node (col. 3, ll. 29-33; col. 4, ll. 52-54), and obtains network characteristics information (e.g., logical entry TCP ports 240, 340 and UDP ports 245, 345[2]) from network equipment connected to the attacked network node (col. 4, ll. 40-44; col. 4, l. 65 to col. 5, l. 2).

[2] As indicated *supra*, Appellants have acknowledged that the ports are logical entry points.

Thereafter, the method and system determines an upstream router (i.e., a physical entry point) that originated the attack upon the network node (col. 3, ll. 29-47) by comparing suspicious instances of intrusion information (e.g., flooding and/or denial of service) with a list of network characteristic information (i.e., the logical entry TCP/IP and UDP ports) (col. 4, ll. 57-59).

Inasmuch as Ricciulli determines a physical entry point of the attack via a comparison of logical entry point network information and intrusion information, and does not determine a logical entry point via a correlation engine, we agree with Appellants' argument (App. Br. 12-20) that Ricciulli does not determine a logical entry point of the attack, and does not identify a physical entry point of the attack associated with the logical entry point as set forth in claim 5 on appeal.

In summary, the anticipation rejection of claims 5 to 10, 15, and 18 to 20 is reversed because each and every limitation in the claims is not found either expressly or inherently in the cited reference to Ricciulli. *In re Crish*, 393 F.3d 1253, 1256 (Fed. Cir. 2004).

The obviousness rejection of claims 11, 17, and 21 to 27 is reversed because Skirmont's teachings of a physical mapping of physical ports to logical ports, and the routing of a physical packet to a physical egress port (col. 4, l. 66 – col. 5, l. 67) do not cure the noted shortcomings in the teachings of Ricciulli.

The obviousness rejection of claim16 is reversed because the network dispatcher router teachings of Hunt do not cure the noted shortcomings in the teachings of Ricciulli.

The decision of the Examiner is reversed.

REVERSED

KIS

Duke Yee
Yee & Associates, P. C.
4100 Aipha Road
Suite 1100
Dallas, TX 75244